1995

Computer-Related Crimes

Michael W. Carroll

COMPUTER-RELATED CRIMES

I. INTRODUCTION

This article tracks developments in computer-related criminal law and legal literature, including an analysis of federal computer crime legislation and enforcement, and a discussion of state and international approaches.

A. Defining Computer Crime

The rapid development of computer technology has spawned a variety of new criminal behaviors and an explosion in specialized legislation to combat

them.[1] While computer crimes include traditional crimes committed with a computer, the term also encompasses offenses against intellectual property and other crimes which do not fall within traditional criminal statutes. Moreover, computer crime is moving in new directions as child pornographers abuse the information highway to distribute their wares and rapists and pedophiles use the internet to meet and set up their victims.[2] The diversity of computer-related offenses thus demands a broad definition. The Department of Justice defines computer crimes as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution."[3]

Estimates of the predominant sources and extent of computer crimes vary. Many experts value losses due to computer crimes in the hundreds of millions and even billions of dollars.[4] While the exploits of youthful computer hackers have received the most press coverage, experts maintain that insider crimes committed by disgruntled or greedy employees have caused far more damage.[5]

Computer crime legislation attempts to respond both to the problems of

---

1. Michael C. Gemignani, *What is Computer Crime, and Why Should We Care?*, 10 U. ARK. LITTLE ROCK L.J. 55, 55-56 (1987-88).

2. Law enforcement officials from Florida to California maintain that opportunities for on-line pedophilia have escalated as both pedophiles and children become more computer literate. Barbara King & Patricia King, *Child Abuse in Cyberspace*, NEWSWEEK, Apr. 18, 1994, at 40. *See also* Laurent Belsi, *The Dark Side of Cyberspace: Virtual Reality Now Harbors Actual Criminals and Addicts Who Shun the World*, CHRISTIAN SCI. MONITOR, July 18, 1994, at 9. In March 1993, in the largest anti-child pornography effort ever undertaken by U.S. law enforcement, 300 local, state, and federal agents served 31 search warrants in 15 states, resulting in six arrests for illegal importation of child pornography from a computer system in Denmark. Marianne Lavelle, *U.S. Sees Computer Crime as Threat*, NAT'L L.J., July 25, 1994, at A21.

3. NATIONAL INSTITUTE OF JUSTICE, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 2 (1989) [hereinafter CRIMINAL JUSTICE RESOURCE MANUAL]. Another broad definition of computer crimes includes any illegal act involving a computer that may be prosecuted under criminal laws. CATHERINE CONLY, ORGANIZING FOR COMPUTER CRIME INVESTIGATION AND PROSECUTION 6 (1989).

4. *The Computer Abuse Amendments Act of 1990: Hearings on 2476 Before the Subcomm. on Technology and the Law of the Sen. Comm. on the Judiciary*, 101st Cong., 2d Sess. 13 (1990) (testimony of Deputy Assistant Attorney General Mark M. Richard) (estimating that computer related crime costs U.S. companies as much as five billion dollars per year). *See also* James Daly, *Virus Vagaries Foil Feds*, COMPUTERWORLD, July 12, 1993, at 1 (citing survey of corporations placing cost to businesses at nearly $2 billion in 1993); William G. Flanagan & Brigid McMenamin, *The Playground Bullies are Learning How to Type*, FORBES, Dec. 21, 1992, at 184 (placing cost estimates of computer crimes at $500 million to $5 billion per year). According to the FBI's National Computer Crime Squad, fraudulent use of computers to access telephone long-distance codes, credit cards, and other computerized records may drain as much as $5 billion from the economy. Gordon Witkin, *Wanted, in Cyberspace*, U.S. NEWS & WORLD REP., Mar. 14, 1994, at 71.

5. Richard C. Hollinger & Lonn Lanza-Kanduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 116-17 (1988); 10 COMPUTER RELATED CRIME: ANALYSIS OF LEGAL POL'Y 33-34 (1986); Douglas M. Reimer, *Judicial and Legislative Responses to Computer Crimes*, 53 INS. COUNS. J. 406, 419 (1986).

old crimes committed with new technology and new types of crimes made possible by new technology. Some efforts to deter computer-related crime have closed loopholes in existing statutes; other statutes function as independent computer crime chapters.[6]

B. Types of Computer-Related Offenses

There is no "typical" computer-related crime and no typical motive for committing such crimes.[7] Computer criminals can be teenage hackers, disgruntled employees, mischievous technicians, or international terrorists.[8] However, it is possible to classify computer-related crimes by considering the role the computer plays in a particular crime.[9]

First, a computer may be the "object"[10] of a crime, meaning the computer itself is targeted. Theft of computer processor time and computerized services are included in this category.

Second, the computer may be the "subject"[11] of a crime. In these cases, the computer is the physical site of a crime, or is the source of or reason for unique forms of assets lost.[12] The use of "viruses"[13] and "logic bombs"[14] fit into this category. These crimes present novel legal problems because of the intangible nature of the electronic information which is the object of the crime.[15]

Third, a computer may be an "instrument"[16] used as a means of commit-

---

6. *See supra* note 5.

7. One commentator has identified six motives for committing computer-related crimes where computers are subjects or objects of crime: (1) to exhibit technical prowess; (2) to highlight vulnerabilities in computer security systems; (3) to punish or retaliate; (4) computer voyeurism; (5) to assert a philosophy of open access to computer systems; (6) to sabotage. Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 24-26 (1990).

8. Some argue that computer offenders are changing from mischievous, thrill-seeking teenagers to criminals intent on making large profits. Flanagan & McMenamin, *supra* note 4, at 184.

9. CRIMINAL JUSTICE RESOURCE MANUAL, *supra* note 3, at 2.

10. *Id.*

11. *Id.*

12. *Id.*

13. A computer "virus" is a program which replicates itself and spreads through a computer system or network. Viruses may be benign or destructive; some cause unexpected screen displays, delete computer files, create false information, or cripple a computer's ability to process information. Camille Cardoni Marion, *Computer Viruses and the Law*, 93 DICK. L. REV. 625, 627 (1989). *See also* Note, *Administering the Antidote to Computer Viruses*, 19 RUTGERS COMPUTER & TECH. L.J. 259, 259 n.4 (1993) (describing and defining computer viruses).

14. "Logic bombs" are destructive programs which are "detonated" by the occurrence of a specific event, such as a particular date or time. *See, e.g.*, United States v. Lauffenberger, No. 91-0594-T (S.D. Cal. 1990) (slip op.) (employee planted a logic bomb in his employer's computer system).

15. Hollinger & Lanza-Kaduce, *supra* note 5, at 103.

16. CRIMINAL JUSTICE RESOURCE MANUAL, *supra* note 3, at 2.

ting traditional crimes such as theft, fraud, embezzlement, or trespass,[17] albeit in a more complex manner.[18] For example, a computer might be used to scan telephone codes automatically in order to make unauthorized use of a telephone system.[19]

II. FEDERAL APPROACHES

A. Federal Criminal Code

Computer-related crimes have been treated as distinct federal offenses since 1984, when Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Law of 1984.[20] Since the 1984 Act was passed, the volume of such legislation has expanded greatly to meet the challenge of more types of computer-related crimes. However, federal computer crime legislation has been inexplicably unresponsive to the problems of fighting computer crime.[21] It began as a piecemeal effort to solve a problem with unknown dimensions and importance.[22] As more data about computer crimes has become available, the law has become more precise.[23] Yet the most recent attempt to address the problem of computer-related crimes, the

---

17. Computer trespass, or "voyeurism," includes intentional, non-malicious, unauthorized access of computer files. Hollinger & Lanza-Kaduce, *supra* note 5, at 103-04.

18. Many traditional crimes, when committed using a computer, have been specially defined in computer-specific federal and state statutes. *See infra* notes 20-47 and accompanying text (federal computer statute includes offenses where computer is an instrumentality) and *infra* notes 122-54 and accompanying text (state statutes).

19. Hollinger & Lanza-Kaduce, *supra* note 5, at 103-04.

20. Pub. L. No. 98-473, 98 Stat. 2190 (1984) [hereinafter the 1984 Act] (codified at 18 U.S.C. § 1030 (1988 & Supp. III 1991)), *amended by* Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified at 18 U.S.C. § 1030 (1988 & Supp. V 1993). For legislative history of the 1984 Act, see H.R. REP. NO. 98-894, 98th Cong., 2d Sess. 9 (1984) (indicating that difficulties in prosecuting computer-related crime arise because the property involved is intangible, making prosecution under theft and larceny statutes difficult). *See also* Note, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER/ L.J. 61, 63-66 (1993) (discussing background of the 1984 Act) [hereinafter *Trespassers Will Be Prosecuted*].

For discussion of federal prosecution of computer crimes prior to 1984, see Note, *Addressing the Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1900-01 (1991) (discussing inadequacies of prosecuting computer-related crime under traditional criminal statutes). *See also* Project, *Computer Crime, Fourth Survey of White Collar Crime*, 24 AM. CRIM. L. REV. 429, 430-432 (1987) (review of pre-1984 federal prosecution of computer-related crime).

21. For an analysis of problems with enforcing computer-crime laws and an argument for alternatives to ex post criminalization of computer crimes, see generally Michael P. Dierks, *Computer Network Abuse*, 6 HARV. J.L. & TECH. 307 (1993).

22. *See* Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 482-83 (1990) (drafting legislation is difficult because of a lack of concrete knowledge about the problem) [hereinafter *A Measured Response*].

23. *Id.* at 483-84 (Computer Fraud and Abuse Act of 1986 sought to increase deterrence of computer crimes affecting compelling federal interests by tightening up statutory language and modifying the elements of existing offenses).

1994 Act, may still contain significant gaps.[24] This section examines the major federal statutes directed at computer-related crimes and some of their practical shortcomings.

1. Computer Fraud and Abuse Act

The 1984 Act was widely criticized for being too ambiguous and narrow in scope to provide adequate protection against computer-related offenses.[25] In an attempt to strengthen and clarify the 1984 Act,[26] Congress amended it in 1986 with the Computer Fraud and Abuse Act.[27]

The 1986 Act was directed at unauthorized intentional access to federal interest computers.[28] The statute proscribes six types of illegal activities.[29] It prohibits unauthorized access of a computer:[30] (1) to obtain information relating to national defense or foreign relations;[31] (2) to obtain information in a financial record of a financial institution or consumer reporting agency;[32] or (3) to manipulate information on a computer that would affect the United

---

24. For example, it is not clear that the Act covers malevolent software. *See* Note, *It's Virus Season Again, Has Your Computer Been Vaccinated? A Survey of Computer Crime Legislation as a Response to Malevolent Software*, 72 WASH. U. L.Q. 411, 438-440 (1994) (discussing application of the 1994 Act in its then-proposed form to creators of computer viruses).

25. Michael Todd Friedman, *Misuse of Confidential Information in Interstate Commerce: How Well Do Our Present Laws Address the Issue?*, 4 SOFTWARE L.J. 529, 548 n.107 (1991). *See also A Measured Response*, *supra* note 22, at 455-456 (describing criticism leading to 1986 amendment).

26. Friedman, *supra* note 25, at 548 n.107.

27. 18 U.S.C. § 1030 (1988 & Supp. V 1993) [hereinafter "the 1986 Act"].

28. 18 U.S.C. § 1030(e)(2) (1988 & Supp. V 1993). "Federal interest computer" is defined as:

> a computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government, and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or which is one of two or more computers used in committing the offense, not all of which are located in the same state.

Id. See also United States v. Fernandez, No. 92-CR-563, 1993 WL 88197 (S.D.N.Y. Mar. 25, 1993) (rejecting the argument that the words "used in committing the offense" in § 1030(e)(2)(B) are unconstitutionally vague because they describe the crime through reference to the offense itself and stating that "Federal interest computer" relates only to the federal courts' jurisdiction).

A "computer" is:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1).

29. 18 U.S.C. § 1030(a)(1)-(6) (1988 & Supp. V 1993).

30. Significant statutory language, including "access," "unauthorized," and "affects the use" remains undefined by both the statute and the limited case law.

31. 18 U.S.C. § 1030(a)(1).

32. 18 U.S.C. § 1030(a)(2). A "financial record" is defined as "information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution." 18

States government's operation of the computer.[33] It also prohibits: (4) accessing a "federal interest computer" without or in excess of authorization and with intent to defraud or obtain anything of value.[34] Subsection (5) of the 1986 Act was amended in 1994, but for those actions governed by the 1986 Act, intentional access of a "federal interest computer" without authorization, and thereby altering, damaging, or destroying information, or preventing "authorized use" of the computer is prohibited.[35] The access must either cause an aggregate loss of $1,000 during a one year period, or actually or potentially modify or impair medical examination, diagnosis, treatment, or care.[36] Finally, the 1986 Act prohibits: (6) "knowingly," and with intent to defraud, trafficking in passwords which either would permit unauthorized access to a government computer, or affect interstate or foreign commerce.[37]

Punishment for an attempt to commit an offense is identical to punishment for commission of the offense itself.[38] The 1986 Act expressly grants investigatory authority to the United States Secret Service, in addition to any other agency having such authority.[39]

2. Computer Abuse Amendments Act of 1994

Responding to criticism of the 1986 Act, Congress passed the Computer Abuse Amendments Act of 1994[40] to broaden the scope of liability for

---

U.S.C. § 1030(e)(5). "Financial institution" is defined as:

> (A) an institution with deposits insured by the Federal Deposit Insurance Corporation;
> (B) the Federal Reserve or a member of the Federal reserve including any Federal Reserve Bank;
> (C) a credit union with accounts insured by the National Credit Union Administration;
> (D) a member of the Federal home loan bank system and any home loan bank
> (E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
> (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
> (G) the Securities Investor Protection Corporation;
> (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978; and
> (I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

18 U.S.C. § 1030(e)(4).

33. 18 U.S.C. § 1030(a)(3).

34. 18 U.S.C. § 1030(a)(4). "[E]xceeding authorized access" is defined as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

35. 18 U.S.C. § 1030(a)(5), *amended by* the Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796, 2097.

36. *Id.*

37. 18 U.S.C. § 1030(a)(6).

38. 18 U.S.C. § 1030(b) (1988 & Supp. V 1993).

39. 18 U.S.C. § 1030(d) (1988 & Supp. V 1993).

40. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796, 2097 (1994) (amending 18 U.S.C. § 1030) [hereinafter the 1994 Act].

computer crimes and to expressly provide civil remedies for the victims of computer crimes. The 1994 Act makes three changes to § 1030(a)(5), broadening the scope of liability. First, the 1994 Act changes coverage from acts committed on federal interest computers and affecting such computers to acts committed on computers used in interstate commerce or communications and affecting any computer.[41] Second, the threshold requirement of "unauthorized access" has been removed.[42] As a result, the class of those potentially liable has been expanded to include, among others, company insiders and users of computer networks, who were arguably immune under the 1986 Act because their access was authorized. Finally, the 1994 Act criminalizes certain types of reckless conduct in addition to intentional acts.[43] This may facilitate prosecution of hackers who cause the transmission of malevolent software, such as computer viruses, if such actions are sufficiently reckless but would not have been considered intentional under the 1986 Act.

Under the amended statute, intentional computer crimes committed on interstate computers are felonies,[44] while reckless acts on interstate computers are misdemeanors.[45] The 1994 Act also provides an incentive for victims to report computer-related crimes by allowing civil remedies for victims of intentional computer crimes.[46] Additionally, the 1994 Act amends subsection

---

41. *Compare* the 1994 Act (amending § 1030(a)(5) to apply to "[whomever] through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information code or command to a computer or computer system . . . .") *with* the 1986 Act (§ 1030(a)(5) reads, "[whoever] . . . accesses a Federal interest computer . . . and . . . alters, damages or destroys information in any such computer . . . .").

42. *Compare* the 1994 Act (amending § 1030(a)(5) to apply to "[whomever] through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information code or command to a computer or computer system . . . .") *with* the 1986 Act (§ 1030(a)(5) reads, "[whoever] intentionally accesses a Federal interest computer without authorization . . . .").

43. 18 U.S.C. § 1030(a)(5)(B)(i). This provision extends liability to whomever, through an interstate computer knowingly transmits a code or command with reckless disregard of a substantial and unjustifiable risk that the transmission will cause damage to or deny access to a computer or computer system. *Id.*

44. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322 § 290001(c)(2), 108 Stat. 1796, 2098 (1994) (amending 18 U.S.C. § 1030(c)(3)(A)).

45. § 290001(c)(4), 108 Stat. at 2098 (amending 18 U.S.C. § 1030(c)(3)(B)).

46. The 1994 Act adds 18 U.S.C. § 1030(g), which provides as follows:

> Any person who suffers damage or loss by reason of a violation of the section, other than a violation of subsection (a)(5)(B) [reckless conduct], may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) [intentional modification or impairment of medical records] or (a)(5)(B)(ii)(II)(bb) [reckless modification or impairment of medical records] are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

§ 290001(d), 108 Stat. at 2098. There is no civil remedy for reckless conduct. However, if the

(a)(3) to insert "adversely" before "affects the use of the Government's operation of such computer",[47] implying that a trespasser might affect the computer benignly and escape prosecution.

3. Other Statutes

Other statutes have been useful in prosecuting computer-related crimes falling outside the Computer Fraud and Abuse Act. Computer-related crimes can be charged under at least forty different federal statutes.[48] What follows is a brief discussion of the statutes most commonly used to prosecute computer-related crimes which are not covered by the Computer Fraud and Abuse Act.[49] Such offenses range from theft of computer software to unauthorized access of a computer system without causing damage.[50]

a. Copyright Act

Any person who unlawfully copies and distributes software may be subject to punishment for criminal copyright infringement.[51] The criminal copyright infringement statute has three elements: (1) infringement of a copyright; (2) done willfully; and (3) for commercial advantage or private financial gain.[52] The first element of copyright infringement may be satisfied by the mere unauthorized copying of computer software, but the second and third elements are often more difficult to prove.[53]

---

amendment is to be read that no civil action may be maintained against a violator of subsection (a)(5)(B), it is unclear why damages for violations of subsection (a)(5)(B)(ii)(II)(bb) may include more than economic damages.

47. § 290001(f), 108 Stat. at 2099 (amending 18 U.S.C. § 1030(a)(3), which applies to intentional and unauthorized access to any government computer where the access "affects the use of the Government's operation of such computer").

48. UNITED STATES SENTENCING COMMISSION, COMPUTER FRAUD WORKING GROUP, REPORT SUMMARY: SUMMARY OF FINDINGS at 3 (1993) [hereinafter REPORT SUMMARY].

49. For additional perspectives on prosecution under other statutes, see generally *Trespassers Will Be Prosecuted, supra* note 20 (discussing application of federal statutes other than the 1986 Act to computer crimes).

50. Stanley S. Arkin et al., PREVENTION AND PROSECUTION OF COMPUTER AND TECHNOLOGY CRIME, 3-20 (1991). *See also* Stephen Fishbein, *What Victims of Computer Crime Should Know and Do*, N.Y.L.J., Nov. 12, 1993, at 1 (for an analysis of how some of these statutes might be applied to computer crimes).

51. 17 U.S.C. § 506(a) (1988 & Supp. V 1993). *See generally Intellectual Property* article in this issue.

52. 17 U.S.C. § 506(a).

53. *Id. Compare* United States v. Hux, 940 F.2d 314 (8th Cir. 1991) (finding copyright infringement where only 205 bytes of defendant's computer program were similar with 16,384 bytes of original program), *overruled in part by* United States v. Davis, 978 F.2d 415 (8th Cir. 1992) (not overruling the holding on the copyright claim, see *infra* note 71) *with* United States v. Goss, 803 F.2d 638 (11th Cir. 1986) (prosecution failed to prove copyright infringement where defendant claimed that video games were legally obtained, thus implicating "first sale" doctrine). *But see* United States v. Cross, 816 F.2d 297, 301 (7th Cir. 1987) (government need not show defendant actually profited, only that infringer intended to make a profit).

b. National Stolen Property Act

The National Stolen Property Act[54] prohibits the transportation in interstate commerce of "any goods, wares, securities or money" valued at $5,000 or more and known to be stolen or fraudulently obtained.[55] This statute has been applied to various computer-related crimes, including fraudulent computerized transfers of funds.[56] The court has held that computer software does not constitute "goods" or "wares" under the National Stolen Property Act, if the programs were solely in an intangible form.[57] The court has also distinguished between the theft of software only, and the theft of software in conjunction with the theft of tangible hardware, which is covered by the terms "goods" and "wares" in the National Stolen Property Act.[58]

c. Mail and Wire Fraud

The federal mail and wire fraud statutes[59] prohibit the use of interstate wire communications and mails to further a fraudulent scheme to obtain money or property.[60] One commentator suggests that these statutes seem to apply to "any computer-aided theft involving the use of interstate wire, the mails or a federally insured bank."[61] Furthermore, any attempt to obtain an unauthorized copy of a computer program in an intangible form may be covered by the mail and wire fraud statutes.[62]

---

54. 18 U.S.C. § 2314 (1988 & Supp. V 1993). *See generally* the *Intellectual Property* article in this issue.

55. 18 U.S.C. § 2314.

56. *See* United States v. Jones, 553 F.2d 351 (4th Cir.) (fraudulent diversion of funds by computer violates National Stolen Property Act), *cert. denied*, 431 U.S. 968 (1977).

57. United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991) (concluding that computer program in source code form is not physical and thus did not constitute "goods" or "wares" under National Stolen Property Act).

58. *See* United States v. Lyons, 992 F.2d 1029, 1033 (10th Cir. 1993) (rejecting defendant's claim that *Brown* precludes consideration of the value of stolen software in determining sentencing under the National Stolen Property Act).

59. 18 U.S.C. §§ 1341, 1343 (1988 & Supp. V 1993). *See generally* the *Mail and Wire Fraud* article in this issue.

60. 18 U.S.C. §§ 1341, 1343.

61. Arkin, *supra* note 50, at 3-77. *See, e.g.*, United States v. Gaind, 31 F.3d 73 (2d Cir. 1994) (government contractor altered computer clocks to "backdate" reports to the Environmental Protection Agency to falsely represent that tests had been completed within specified period); Mid Atlantic Telecom, Inc. v. Long Distance Servs., Inc., 18 F.3d 260 (4th Cir. 1994) (civil action under RICO based on violations of §§ 1341 and 1343 where reseller of long distance telephone service used computer program to randomly add minutes to calls of customers); United States v. De Biasi, 712 F.2d 785 (2d Cir.) (credit card fraud involving interstate computer transmission), *cert. denied*, 464 U.S. 962 (1983); United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) (former employee's unauthorized attempt to access computer to obtain company property), *cert. denied*, 441 U.S. 922 (1979); United States v. Upton, 856 F. Supp. 727 (E.D.N.Y 1994) (defendants falsified computer transactions regarding airplane maintenance).

62. Arkin, *supra* note 50, at 3-33. *See also* Carpenter v. United States, 484 U.S. 19, 27-28 (1987) (intangible property is covered by federal mail and fraud statutes).

d. Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986[63] (ECPA) updated the federal law pertaining to wire and electronic communications interception[64] to prohibit unauthorized interception of computer communications.[65] Additionally, it created a new offense of obtaining, altering, or preventing authorized access to data stored electronically in a facility through intentional, unauthorized access of the facility.[66] It is not always clear which provisions of the ECPA cover electronic communication such as electronic mail, which is both transmitted and stored.[67] The offense created by section 2701 seems to provide additional deterrence to hackers, although there have been no successful prosecutions under the statute.[68]

The ECPA was intended to prevent hackers from intercepting computer communications by: (1) expanding the protection of individuals' privacy;[69] and (2) expanding the number of crimes that can be investigated through electronic surveillance methods.[70] Although no courts have interpreted the ECPA as it relates to computer crimes, in the arguably analogous context of modification of satellite television descramblers, the majority favor a broad interpretation of the ECPA.[71] Thus, the statute may also be interpreted broadly to apply to computer-related crime. Section 2707(a) provides for civil damages for violation of section 2701, and it is possible that governmental "entities" may fall within the scope of civil liability.[72]

---

63. 18 U.S.C. §§ 2510-2520, 2701-2710 (1988 & Supp. V 1993) ("ECPA").

64. 18 U.S.C. §§ 2510-2520 (1988 & Supp. V 1993).

65. 18 U.S.C. § 2511(1) (1988 & Supp. V 1993), *as amended by* Pub. L. No. 103-322, § 320901, 108 Stat. 1796, 2123 (1994).

66. 18 U.S.C. § 2701 (1988 & Supp. V 1993).

67. *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994) (holding that government seizure of a computer used to operate an electronic bulletin board, and containing private electronic mail that had been sent to (stored on) the bulletin board but not read (retrieved) by the intended recipient, was not an "interception" under § 2510 of the ECPA).

68. *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432, 442 (W.D. Tex. 1993) (affidavit supporting warrant to seize information from computer bulletin board was inadequate under 18 U.S.C. § 2703(d)), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

69. 18 U.S.C. § 2510(1) (1988 & Supp. V 1993).

70. 18 U.S.C. § 2516 (1988 & Supp. V 1993). *See also* Arkin, *supra* note 50, at 9-11.

71. *See* United States v. One Macom Video Cipher II, 985 F.2d 258 (6th Cir. 1993) (neither § 2111 nor § 2512 of the ECPA nor 47 U.S.C. § 605 excludes modification of satellite descramblers from coverage); United States v. Harrell, 983 F.2d 36 (5th Cir. 1993) (ECPA applies to modified satellite descramblers); United States v. Davis, 978 F.2d 415 (8th Cir. 1992) (overruling United States v. Hux, 940 F.2d 314 (8th Cir. 1991), with respect to its holding that manufacture of satellite descrambler was not a violation of § 2512(1)(b)); United States v. Lande, 968 F.2d 907 (9th Cir. 1992) (modification of descrambler is covered by ECPA); United States v. Splawn, 963 F.2d 295 (10th Cir. 1992) (same). *But cf.* United States v. Herring, 933 F.2d 932 (11th Cir. 1991), *vacated*, 977 F.2d 1435 (11th Cir. 1992) ("satellite cable programming" as defined in 47 U.S.C. § 605 is excluded from coverage of the ECPA).

72. *See* Organizacion JD LTDA v. U.S. Dept. of Justice, 18 F.3d 91, 94-95 (2d Cir. 1994) (per

B. Enforcement Strategies

Although federal computer crime laws were drafted to aid prosecutors, there have been few indictments under these laws. The 1984 Computer Abuse Act resulted in only one prosecution.[73] Between January 1989 and April 1993, there were only seventy-six convictions under 18 U.S.C. § 1030.[74] Of the fifty cases studied, more than half were convictions for general fraud under § 1030(a)(4).[75]

The reason for the scarcity of prosecutions under the 1984 and 1986 Acts is unclear, but two possible causes warrant consideration. First, there are not many reported instances of computer crimes involving "federal interest" computers. Furthermore, owners of large federal interest computers may prefer to handle security problems themselves to avoid the embarrassment of a public trial focusing on the vulnerability of their computers.[76] It remains to be seen whether the broadened scope of the 1994 Act and its provision of civil remedies will lead to increased prosecution. Second, computer crimes which might be characterized as federal crimes may instead be prosecuted under state computer crime laws. As more people are successfully prosecuted under state computer crime law, prosecutions in the federal sphere may be encouraged.[77]

While the volume of computer-crime prosecution is low, recent trends

---

curiam) (governmental "entities" are subject to liability under § 2707(a) and remanding where appellants were intended recipients of electronic fund transfers that were seized by DEA agents as proceeds of illegal money-laundering and narcotics transactions); *see also* United States v. Daccarett, 6 F.3d 37 (2d Cir. 1993) (related case arising under the same facts holding that seizures of EFTs were not "interceptions" under the ECPA because no "device" was used, as required by 18 U.S.C. § 2510(4)), *cert. denied*, 114 S. Ct. 1294 (1994).

73. *See* Joseph B. Thompkins, Jr. & Frederick S. Ansell, *Computer Crime: Keeping Up with High Tech Criminals*, 1 CRIM. JUST. 30, 32 (1987) (discussing United States v. Fadriquela, No. 85-CR-40 (D. Colo. 1985)).

74. REPORT SUMMARY, *supra* note 48, at 3. *See, e.g*, United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (upholding defendant's conviction under § 1030(a)(5) for introducing a "worm" into the federal Internet computer network, jamming up to 6,000 federal and federal interest computers across the country), *cert. denied*, 502 U.S. 817 (1991); United States v. Wittman, No. 91-CR-327 (D. Colo. 1991) (defendant pled guilty to accessing and damaging data in a NASA computer without authorization, violating § 1030(a)(5)); United States v. Lauffenberger, No. 91-0594-T (S.D. Cal. 1990) (employee pled guilty to attempted computer tampering of employer's federal interest computer, in violation of § 1030(a)(5)(A), 1030(b)).

75. REPORT SUMMARY, *supra* note 48, at 3-4.

76. One commentator has suggested that the Computer Fraud and Abuse Act be amended to require businesses and others to report computer crimes committed against them. In addition, a provision allowing civil remedies and restitution, (as was adopted in the 1994 Act [see *supra* note 46]), would provide additional incentives for victims to report computer crimes. *A Measured Response*, *supra* note 22, at 487-89. *See also* S. 8, 103d Cong., 1st Sess. (1993) (proposing civil remedies in computer crime cases); H.R. 2847, 103d Cong., 1st Sess. (1993) (providing civil remedies for federal computer offenses under 1986 Act).

77. *See infra* notes 122-54 and accompanying text (summary of state computer crime statutes).

indicate that federal authorities are taking steps to raise the profile of computer-crime prosecution.[78] Enforcement against well-known hackers appears to be on the rise.[79] In addition, federal prosecutors are securing controversial indictments for computer crimes under a broad reading of wire fraud and criminal copyright infringement statutes.[80] Finally, the proliferation of computer bulletin boards has led to prosecution of illegal distribution

---

78. For a profile of some recent cases involving the Internet, *see* Michael Meyer & Anne Underwood, *Crimes of the 'Net'*, NEWSWEEK, November 14, 1994, at 46. In the largest enforcement action to date, "Operation Sundevil", the Department of Justice and the Secret Service launched a nationwide crackdown on telephone and credit card fraud involving stolen card numbers and customer access codes from national telephone and credit card computer networks. *See* Marc Rotenberg, *Let's Look Before We Legislate*, COMPUTERWORLD, October 21, 1991, at 25 (calling for a congressional hearing to assess "Operation Sundevil"); Mark Lewyn & Evan Schwartz, *Why 'The Legion of Doom' Has Little To Fear of the Feds*, BUSINESS WEEK, April 15, 1991, at 31 (concerning setbacks in "Operation Sundevil"). The investigation covered 14 cities and resulted in the seizure of some 23,000 computer disks. The first conviction in this case did not come until February 1992, when a suspect pleaded guilty to possession of illegal telephone access codes. *Operation Sundevil Nabs First Suspect; Defendant Pleads Guilty To Possession of Access Codes, Faces 10-Year Term*, COMPUTERWORLD, Feb. 17, 1992, at 15.

However, in Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994), the district court found that the officers' zeal exceeded their statutory authority when they seized documents and information from the company. The officers also failed to promptly return information protected by the Stored Wired and Electronic Communications and Transactional Records Access Act. *Id.* at 440 n.7. The company successfully sued the Secret Service, recovering expenses and economic damages. *Id.* at 438.

79. An employee of MCI Communications Corp., known as Knight Shadow, was charged with stealing more than 50,000 telephone calling-card numbers that were eventually sold in the United States and Europe and were used to make more than $50 million worth of phone calls, many of them to computer bulletin boards. Sandra Sugawara, *Arrest Made in Calling Card Fraud*, WASH. POST, October 4, 1994, at C1.

Two members of a computer-based conspiracy to win radio contest prizes that included new cars and trips to Hawaii were convicted in 1994. Dark Dante, who led the conspiracy, pled guilty to single counts of conspiracy, computer fraud, mail fraud, obstructing justice and money laundering, and two counts of intercepting a wire communication. *Guilty Plea Entered in Radio Contest Conspiracy*, L.A. TIMES, June 15, 1994, at B2. In August 1994, Agent Steal, who had been convicted and had fled prior to sentencing was apprehended by an FBI agent. John Johnson, *FBI Footwork Puts Computer Hacker in Jail*, L.A. TIMES, August 30, 1994, at B1.

Another well-known hacker who was arrested and convicted of computer crimes in 1988, Condor, is the subject of an FBI investigation for unauthorized entry into Pacific Bell Telephone Co. computers. John Johnson & Julie Tamaki, *Authorities Again Seek Legendary Hacker*, L.A. TIMES, July 10, 1994, at B2.

80. A student at the Massachusetts Institute of Technology was indicted on one count of conspiracy to commit wire fraud for allegedly operating an electronic bulletin board on MIT computers that allowed users to exchange more than $1 million worth of copyrighted software. Elisha King, *Man Accused of Software Theft MIT Student Allegedly Used School Computer to Aid Illegal Copying*, WASH. POST, April 9, 1994, at G4. While he apparently did not attempt to sell copyrighted software, others have. "One of the first successful criminal prosecutions involving network software copyright infringement" involved an individual who sold illegal copies of Novell's NetWare net operating system. Bob Brown, *Novell Helps Feds Win Case Against Copyright Violator*, NETWORK WORLD, April 27, 1992, at 25; *see* Barbara Carton, *Man Charged in Software Piracy*, BOSTON GLOBE, September 1, 1994, at Bus. 41 (man charged with conspiracy and criminal copyright infringement for allegedly distributing copyrighted software to his bulletin board subscribers).

of computerized pornographic materials[81] and of computer-related sexual assault on minors.[82]

In late 1991, the Department of Justice established the Computer Crime Unit ("CCU") within the Criminal Division. The CCU was given the responsibility for prosecuting computer crimes, lobbying for strengthened penalties, and pushing for expanded coverage of the federal computer crime statutes.[83] However, there have been only two reported judicial opinions under the 1986 Act since the new Computer Crime Unit was established.[84]

C. Defenses

There are a variety of defenses available under 18 U.S.C. § 1030, including defenses relating to jurisdiction, statutory interpretation, damages, and intent.

For acts covered by the 1986 Act, a federal interest computer must be used and affected. If an individual installs a virus that damages a network without federal interest computers, that person's conduct is not covered by the federal statute.[85] Even under the broadened scope of subsection (a)(5), it is not clear when a computer is "used in interstate commerce or communications."

Defenses to charges under the 1986 Act can also focus on undefined portions of the statutory language.[86] However, in *United States v. Morris*,[87] the only case to give a detailed interpretation of the 1986 Act, the Second Circuit

---

81. *See, e.g., Computer Porn Nets Prison Terms*, WASH. POST, Dec. 3, 1994, at C3 (California couple charged in Tennessee for sending pornographic images over a computer sentenced to at least two and a half years); Adam S. Bauman, *Felony Charges Are Filed Over Porn Cache at Livermore Lab*, L.A. TIMES, Aug. 18, 1994, at D5 (two employees of the Lawrence Livermore National Laboratory loaded computerized pornographic images onto an on-line service); *2 Convicted of Hi-Tech Porn Peddling*, S.F. CHRONICLE, July 29, 1994, at A5 (couple convicted of 11 counts of transmitting obscenity through interstate phone lines via their members-only bulletin board). *See also infra* part V. of this article (prosecution for on-line pornography).

82. *See, e.g., Computer Pedophile Link Feared*, NEWSDAY, Oct. 7, 1994, at A5 (pedophiles use computer bulletin boards to meet victims); Sandy Rovner, *Molesting Children by Computer*, WASH. POST, Aug. 2, 1994 at Z15 (minors give out information on bulletin boards that makes them vulnerable to assault).

83. Michael Alexander, *Justice Revs Up Battle on Computer Crime*, COMPUTERWORLD, Oct. 7, 1991, at 4.

84. *See* United States v. Brady, 13 F.3d 334 (10th Cir. 1993) (defendant altered cellular telephone to gain unauthorized access to telephone services in violation of 18 U.S.C. § 1029(a)); United States v. Sykes, 4 F.3d 697 (8th Cir. 1993) (defendant pleaded guilty to computer access fraud under 18 U.S.C. § 1030(a)(4) for unauthorized use of an automatic teller machine).

85. *See* 18 U.S.C. § 1030 (a)(6)(A) (1988 & Supp. V 1993) (limiting the statute's reach to any computer accessed without authorization which affects interstate or foreign commerce or any computer used by or for the United States Government).

86. 18 U.S.C. § 1030(a)(5). *See supra* notes 28-34 and accompanying text (listing defined and undefined statutory terms).

87. 928 F.2d 504 (2d Cir. 1991).

rejected a defense based on ambiguities in the statutory language.[88] The 1994 Act may have closed some of the loopholes if courts interpret it to reach programmers who introduce a virus into a network by giving an innocent third party an infected program[89] as being sufficiently "reckless."

Another defense to charges under either the 1986 Act or the 1994 Act is that the requisite $1,000 loss did not occur. Neither the 1986 Act nor the *Morris* court articulated how to calculate this loss.[90] Moreover, it is unclear whether there is a loss if malevolent software, such as a virus, does not destroy files, but simply overloads the network, thus slowing down processing speed or using up some of a system's underutilized capacity.[91] Even if a dollar value can be attached to a loss, there is still some question whether one can aggregate losses or whether there must be $1,000 worth of damage at one particular site.[92]

Another available defense under both the 1986 Act and the 1994 Act is that a defendant lacked the requisite intent. The intent defense to charges

---

88. Morris was prosecuted for releasing a "worm" into a computer network, which spread to thousands of other computers and prevented access by duplicating itself so many times that the computer crashed. *Id.* at 505-06. He argued that under § 1030(a)(5) of the 1986 Act, the government was required to prove not only that he intended unauthorized access to a federal interest computer, but also that he intended to prevent others from accessing the federal interest computer. Since he possessed authorized access to the computer, he argued that he could not be prosecuted under the statute because his only wrong was to exceed the scope of his authorization. *Id.* at 511. The Second Circuit, based on its reading of the legislative history, rejected this argument. The court found that the drafters of the Act, cognizant that people with authorized access to a federal interest computer might try to gain unauthorized access to other federal interest computers, did not intend for authorization for some federal interest computers to constitute authorization for all federal interest computers. *Id.* Thus the statute applied to Morris, although the court noted that this defense was not categorically invalid, since a situation could arise which "falls within a nebulous area in which the line between accessing [a computer] without authorization and exceeding authorization might not be clear . . . ." *Id.*

89. Since the 1986 Act required that the defendant illegally access a computer, it did not reach this activity. *Id.*

90. The court in *Morris* stated that the worm affected computers at "numerous installations" and that fixing the problem cost anywhere from $200 to $53,000. *Id.* at 506.

91. Some of these questions may have been answered in *Morris*, where the court "accepted the government's view that 1986 amendments to the [Computer Fraud and Abuse Act] eliminated any distinction between a break-in that damages files or steals money and what Morris was found guilty of, intentional unauthorized access that prevented authorized use." Harold L. Burstyn, *Computer Whiz Guilty*, 76 A.B.A. J. 20 (1990).

92. *See* Michael C. Gemignani, *Viruses and Criminal Law*, 32 COMMUNICATIONS OF THE ACM 669 (1991) (discussing loopholes in the federal Computer Fraud and Abuse Act).

In one instance, a defense based solely on questioning the method for determining losses proved successful. In 1990, a college student faced up to sixty years in prison and a fine of up to $122,000 in connection with charges that he published a purloined electronic memo about a telephone company's 911 system. Rosalind Resnick, *The Outer Limits*, NAT'L L.J., Sept. 16, 1991, at 32. The telephone company, by factoring in hardware expenses, software expenses, and administrative costs, valued the file at $79,000. *Dispute Over Hacked Bell South 911 Document Lingers in Tex. Case*, COMM. DAILY, Sept. 9, 1991, at 2. Later, after it emerged that the same information that was in the memo was available to the public in non-computerized form for about twenty dollars, the charges were dropped. *Id.*

under the 1986 Act has been narrowed by limiting the issue to the intent to access the computer.[93] Although one criticism of the 1986 Act is that the "knowingly" or "intentionally" standard of intent[94] is "the wrong criminal mental state" for prosecuting computer viruses.[95] In *Morris*, the Second Circuit rejected the contention that the adverb "intentionally" in the 1986 Act requires both intentional access and intentional harm; all that is required is intentional access.[96] As a result, once intentional access is proven, courts will probably reject a defense claiming that the effects of a program exceeded the programmer's intentions. The 1994 Act affirms the *Morris* holding by criminalizing certain reckless conduct.[97]

D. Sentencing

1. Computer Fraud and Abuse Act

Subsection (c) sets forth the punishment for an offense under the 1986 Act. Punishment depends on which specific prohibited act was committed under subsections (a) and (b).[98]

The Federal Sentencing Guidelines provide an additional framework for punishing violations under sections 1030(a) and (b) of the 1986 Act.[99] These guidelines determine the base offense level for violations of sections 1030(a)(1),[100] 1030(a)(2)-(6),[101] and 1030(b).[102] Only occasionally do, courts

---

93. *Morris*, 928 F.2d at 507. Morris argued that he had no intent to create a virus which would harm computer networks; he only intended to create a program which would spread innocuously through the network to many computers. *Id.* His experiment went awry, however, when the program began to duplicate itself uncontrollably, crashing thousands of computers. *Student Tells How "Worm" Went Wild*, L.A. TIMES, Jan. 19, 1990, at A4.

94. 18 U.S.C. § 1030(a) (1988 & Supp. V 1993).

95. *See* Raymond L. Hansen, *The Computer Virus Act of 1989: The War Against Computer Crime Continues* 3 SOFTWARE L.J. 717, 734 n.76 (1990) ("knowing" or "intentional" standard means that the defendant must have intent to cause a particular result).

96. United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991).

97. 18 U.S.C. § 1030(a)(5)(B)(i) (1988 & Supp. V 1993).

98. 18 U.S.C. § 1030(c) (1988 & Supp. V 1993).

99. United States Sentencing Commission, *Guidelines Manual*, App. A (Nov. 1994). *See also* U.S.S.G. Ch. 3 (setting forth criteria for upward and downward adjustments of offense levels).

100. 18 U.S.C. § 1030(a)(1) (1988 & Supp. V 1993). The Guidelines set the base offense level for § 1030(a)(1) at 35 if the information is top secret, and at 30 for all other information. U.S.S.G. § 2M3.2(a).

101. 18 U.S.C. § 1030(a)(2)-(6) (1988 & Supp. V 1993). The base offense level for a violation of § 1030(a)(2)-(6) is dependant on the value of the loss suffered. U.S.S.G. § 2F1.1. For a complete explanation of the application of § 2F1.1, see the *Mail and Wire Fraud* article in this issue. *See e.g.* United States v. Lewis, 833 F.2d 76 (6th Cir 1989) (sentence of two years imprisonment imposed for a violation of § 1030(a)(4)).

102. 18 U.S.C. § 1030(b) (1988 & Supp. V 1993). Defendants convicted of § 1030(b) violations receive a base offense level from the guideline for the substantive offense, plus any adjustments from such guideline that can be established as reasonably applicable. U.S.S.G. § 2X1.1(a). Additionally, § 2X1.1(b) delineates possible reductions in the base offense level.

depart from the Guidelines when sentencing a defendant for a violation of the 1986 Act.[103]

2. Other Statutes

a. Copyright Act

The punishment for criminal copyright infringement is set forth in section 2319 of title 18.[104] Section 2319(b) provides variable prison terms and fines for copyright infringements through the reproduction or distribution of phonorecords.[105] First-time offenders who sell more than 10 copies or phonorecords of a copyrighted work within an 180-day period, could face up to five years in prison; subsequent offenders can face up to ten years imprisonment.[106]

Defendants convicted of criminal copyright infringement are sentenced under § 2B5.3.[107] The base offense level is six.[108] If the retail value of the infringing items exceeds $2,000, then the offense level is increased by the corresponding number of levels from the table in § 2F1.1.[109]

b. National Stolen Property Act

Available punishments for a violation of the National Stolen Property Act include a fine of not more than $10,000, imprisonment of not more than ten years, or both.[110] Defendants convicted of violating the National Stolen Property Act are sentenced under § 2B1.1.[111] The base offense level of four is based upon a total loss to the victim of $100.[112] The offense level is raised as the financial loss to the victim increases, up to a maximum increase of twenty offense levels for a loss exceeding $80,000,000.[113] If the offense involved more than minimal planning, the offense level is increased by two levels.[114] Additionally, if the defendant is a person in the business of receiving and selling stolen property, the offense level is increased by four levels.[115]

---

103. *See, e.g.*, United States v. Riggs, 967 F.2d 561 (11th Cir. 1992) (departing upward from sentencing guideline for violation of § 1030 and requiring period of supervised use of computers, where the defendant had committed similar, prior crimes.)

104. 18 U.S.C. § 2319 (1988 & Supp. V 1993).

105. 18 U.S.C. § 2319(b)(1)-(3) (1988 & Supp. V 1993).

106. 18 U.S.C. § 2319(b)(1). *See* U.S.S.G. § 2B5.3.

107. U.S.S.G. App. A.

108. U.S.S.G. § 2B5.3(a).

109. U.S.S.G. § 2B5.3(b)(1).

110. 18 U.S.C. § 2314 (1988 & Supp. V 1993).

111. U.S.S.G. App. A.

112. U.S.S.G. § 2B1.1.

113. U.S.S.G. § 2B1.1(b).

114. U.S.S.G. § 2B1.1(b)(5)(A).

115. U.S.S.G. § 2B1.1(b)(5)(B).

c. Mail and Wire Fraud

Violations of the mail and wire fraud statutes are punishable by fines of up to $1,000, imprisonment of up to 10 years, or both.[116] If the violation affects a financial institution, the punishment is a fine of not more than $1,000,000, imprisonment of not more than thirty years, or both.[117]

d. Electronic Communications Privacy Act

Punishments for violations of the Electronic Communications Privacy Act is provided in 18 U.S.C. sections 2511 and 2701. A violation of section 2511(1) will result in a fine, imprisonment for not more than five years, or both.[118] For first-time offenders under section 2511(4)(a), when the statute is violated for purposes other than for financial gain and the illegally received communication is not scrambled or part of a cellular telephone communication, punishment is limited to imprisonment of not more than one year, and a fine not exceeding $500.[119]

If violation of section 2710(a) is for financial gain, a first time offender shall be fined not more than $250,000, imprisoned for not more than one year, or both. A repeat offender shall be fined according to title 18, imprisoned for not more than two years, or both.[120] Other violations of section 2701(a) result in a maximum fine of $5,000, maximum imprisonment of six months, or both.[121]

III. STATE APPROACHES

A. Overview of State Criminal Codes

Since attempts to apply general criminal codes to computer-related offenses were largely unsuccessful,[122] and because of the serious economic

---

116. 18 U.S.C. §§ 1341, 1343 (1988 & Supp. V 1993).

117. *Id.* The applicable Guideline provisions are § 2C1.7 and § 2F1.1. U.S.S.G. App. A. For a complete explanation of these provisions, see the *Mail and Wire Fraud* article in this issue.

118. 18 U.S.C. § 2511(4)(a) (1988 & Supp. V 1993). Under the Guidelines, defendants convicted of intercepting communications or eavesdropping receive a base offense level of nine. U.S.S.G. § 2H3.1(a). If the purpose of the conduct was to obtain direct or indirect commercial advantage or economic gain, the offense level is increased by three levels. U.S.S.G. § 2H3.1(b)(1). Additionally, if the purpose of the conduct was to facilitate another offense, the guidleline applicable to an attempt to commit that offense should be applied if the resulting offense level would be greater. U.S.S.G. § 2H3.1(c)(1).

119. *Id.* 18 U.S.C. § 2511(4)(b) (1988 & Supp. V 1993). Interception of a radio communication that is not scrambled and is intended for retransmission to the public is not punishable under this section. *Id.* § 2511(4)(c).

120. 18 U.S.C. § 2701(b)(1) (1988 & Supp. V 1993).

121. 18 U.S.C. § 2701(b)(2) (1988 & Supp. V 1993).

122. *See* Jerome Y. Roache, *Computer Crime Deterrence*, 13 AM. J. CRIM. L. 391, 399-401 (1986).

threats posed by such crime, states began to enact statutes specially drafted for the emerging computer technologies.[123] The first specialized computer crime statute was enacted in Florida in 1978. Since then, every state except Vermont has enacted some form of computer-specific criminal statute.[124]

The author catalogs traditional criminal law theories used to combat computer-related crimes and demonstrates the ineffectiveness of each:

> Larceny—When programs or data are copied, but not deleted, from a computer, it is unclear whether property was wrongfully "taken."
>
> Burglary—Requires a physical intrusion into a building, which is not necessary when computers may be accessed remotely.
>
> Embezzlement—Of limited use in computer context, because offense requires that the perpetrator initially has lawful possession or access to the system.
>
> Malicious or criminal mischief—Damage must impair the utility of property or diminish its value. Monetary value of damage due to computer break-ins is often negligible or impossible to determine.
>
> Theft of services—As above, theft of computer services may have a minimal permanent impact on the computer system. Courts generally require a substantial showing of injury.

Id. But see Hancock v. State, 402 S.W.2d 906 (Tex. Crim. App. 1966), (finding that commercial computer programs constituted "property" for purposes of the state's theft statute). Despite the existence of statutes directed specifically at computer-related crime, some offenses are still prosecuted under other statutes. *Cf.* State v. Smith, 798 P.2d 1146 (Wash. 1990) (federal copyright law did not preempt prosecution under state theft statute for unauthorized copying of computer software).

123. The Arkansas state legislature stated its purpose in passing its computer-related crimes statute:

> It is found and determined that computer-related crime poses a major problem for business and government; that losses for each incident of computer-related crime are potentially astronomical; that the opportunities for computer-related crime in business and government through the introduction of fraudulent records into a computer system, the unauthorized use of computers, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; that computer-related crime has a direct effect on state commerce; and that, while various forms of computer-related crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a statute be enacted which deals directly with computer-related crime.

ARK. CODE ANN. § 5-41-101 (Michie 1993). *See also supra* note 4 and accompanying text (discussing the economic impact of computer-related crime).

Some states also recognized the threat to privacy interests. *See* CAL. PENAL CODE § 502 (Deering 1983 & Supp. 1995) ("The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.").

124. ALA. CODE §§ 13A-8-100 to -103 (1994); ALASKA STAT. §§ 11.46.200(3), 11.46.740 (1989); ARIZ. REV. STAT. ANN. § 13-2316 (1989 & Supp. 1994); ARK. CODE ANN. §§ 5-41-101 to -107 (Michie 1993); CAL. PENAL CODE § 502 (Deering 1983 & Supp. 1994); COLO. REV. STAT. §§ 18-5.5-101 to -102 (1990 & Supp. 1994); CONN. GEN. STAT. §§ 53a-250 to -261 (1993); DEL. CODE ANN. tit. 11, §§ 931-939 (1987 & Supp. 1994); FLA. STAT. ch. 815.01-.07 (1993 & Supp. 1994); GA. CODE ANN. §§ 16-9-90 to -94 (1992); HAW. REV. STAT. §§ 708-890 to -893 (1985 & Supp. 1992); IDAHO CODE §§ 18-2201 to -2202 (1987); 720 ILCS 5/16D-1 to -7 (formerly ILL. REV. STAT. ch. 38, para. 16D-1 to -7) (1993); IND. CODE ANN. §§ 35-43-1-4, 35-43-2-3 (1993); IOWA CODE §§ 716A.1 to .16 (1993); KAN. STAT. ANN. § 21-3755

The precise definitions and penalties in these specialized provisions offer significant advantages over general criminal codes by explicitly addressing the unique issues posed by computer crimes, thereby promoting computer security, enhancing deterrence, and facilitating prosecution.[125] Recent reforms in state computer crime statutes have featured provisions expanding forfeiture of computer equipment used in crimes, with several states enacting provisions which allow state authorities to seize property involved in computer crimes.[126]

Other states have recognized that catching and prosecuting computer criminals may be much more difficult than preventing computer crimes. For instance, Nebraska's computer crime statute provides incentives for potential victims of computer crimes to implement their own security measures.[127] Arkansas, Georgia, Oklahoma, and Rhode Island, among others, have statutes encouraging victims of computer crimes to come forward by providing a civil cause of action for compensatory damages.[128]

(Supp. 1993); KY. REV. STAT. ANN. §§ 434.840 to .860 (Michie/Bobbs-Merrill 1985); LA. REV. STAT. ANN. §§ 14:73.1 to .5 (West 1986 & Supp. 1994); ME. REV. STAT. ANN. tit. 17-A, §§ 431-433 (West Supp. 1994); MD. ANN. CODE art. 27, § 146 (1993); MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1990); MICH. COMP. LAWS ANN. §§ 752.791 to .797 (West 1991); MINN. STAT. §§ 609.87 to .891 (1992 & Supp. 1993); MISS. CODE ANN. §§ 97-45-1 to -13 (1994); MO. REV. STAT. §§ 569.093 to .099 (1986 & Supp. 1993); MONT. CODE ANN. §§ 45-6-310 to -311 (1993 & Supp. 1994); NEB. REV. STAT. §§ 28-1343 to -1348 (1989 & Supp. 1994); NEV. REV. STAT. ANN. §§ 205.473 to .490 (Michie 1992); N.H. REV. STAT. ANN. §§ 638:16 to :19 (1986); N.J. REV. STAT. §§ 2C:20-23 to -34 (Supp. 1994); N.M. STAT. ANN. §§ 30-45-1 to -7 (Michie 1989); N.Y. PENAL LAW §§ 156.00 to .50 (McKinney 1988 & Supp. 1995); N.C. GEN. STAT. §§ 14-453 to -457 (1994); N.D. CENT. CODE § 12.1-06.1-08 (1985 & Supp. 1993); OHIO REV. CODE ANN. § 2913.04 (Anderson 1993); OKLA. STAT. tit. 21, §§ 1951-1958 (Supp. 1995); OR. REV. STAT. §§ 164.125, 164.377 (1990 & Supp. 1994); 18 PA. CONS. STAT. § 3933 (Supp. 1994); R.I. GEN. LAWS §§ 11-52-1 to -8 (1994); S.C. CODE ANN. §§ 16-16-10 to -40 (Law. Co-op. 1985 & Supp. 1993); S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to -8 (1983 & Supp. 1994); TENN. CODE ANN. §§ 39-14-601 to -603 (1991 & Supp. 1994); TEX. PENAL CODE ANN. §§ 33.01 to .05 (West 1994); UTAH CODE ANN. §§ 76-6-701 to -705 (1990 & Supp. 1994); VA. CODE ANN. §§ 18.2-152.1 to .14 (Michie 1988 & Supp. 1994); WASH. REV. CODE §§ 9A.52.110 to .130 (1992 & Supp. 1994); W. VA. CODE §§ 61-3C-1 to -21 (Michie 1992); WIS. STAT. § 943.70 (Supp. 1994); WYO. STAT. §§ 6-3-501 to -505 (1988).

125. Roache, *supra* note 122, at 392. Computer security is enhanced because potential victims of computer crimes are more aware of specific possible violations, potential violators are more likely to know which particular activities are unlawful, and prosecution is aided by eliminating the need for prosecutors, attorneys, and judges to rationalize the application of a traditional criminal law in a technical, computer-related context. *Id.*

126. *See, e.g.*, CAL. PENAL CODE § 502.01 (Deering 1983 & Supp. 1995); 720 ILCS 5/16D-6 (1993); N.M. STAT. ANN. § 30-45-7 (Michie 1989). Illinois' provision distributes half the forfeited proceeds to the local government agency which investigated the computer fraud, for training and enforcement purposes, and half to the county in which the prosecution was brought, where it is placed in a special fund and appropriated to the State's Attorney for use in training and enforcement.

127. NEB. REV. STAT. § 28-1343(5) (1989 & Supp. 1994) (a "computer security system" is "a computer program or device that . . . [i]s intended to protect the confidentiality and secrecy of data and information stored in or accessible through the computer system and [d]isplays a conspicuous warning to a user that the user is entering a secure system or requires a person seeking access to knowingly respond by use of an authorized code to the program or device in order to gain access").

128. ARK. CODE ANN. § RM5-41-106 (Michie 1993); GA. CODE ANN. § 16-9-93 (1992); OKLA. STAT.

One commentator has discerned the following ten areas addressed by state computer crime statutes:[129]

> 1. *Expansion of the traditional concept of property.* These statutes attack computer-related crimes by expanding the traditional notion of "property" to include electronic and computer technologies.[130]
> 2. *Destruction.* Many states criminalize acts which "alter, damage, delete or destroy computer programs or files."[131]
> 3. *Aiding and abetting.* Some statutes prohibit use of a computer to facilitate the commission of a crime such as embezzlement or fraud.[132]
> 4. *Crimes against intellectual property.* This type of statute defines new offenses in terms that are analogous to trespassing (unauthorized computer access), vandalism (maliciously altering or deleting data), and theft (copying programs or data). No actual damage is required to prosecute under such a statute.[133]

---

tit. 21 § 1955 (Supp. 1995); R.I. GEN. LAWS § 11-52-6 (1994). *See* Blue Cross & Blue Shield of Connecticut, Inc. v. DiMartino, No. 30-06-42, 1991 LEXIS 1570 (Conn. Super. Ct. July 2, 1991) (plaintiff entitled to any actual damages suffered as a result of defendant's unauthorized removal from computer system of thousands of pages of documents containing information concerning a vast number of accounts, trebled because defendant's conduct was willful and malicious; however, no recovery awarded because no actual damages proven).

129. Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 32-36 (1990). For a detailed analysis of the statutory language in state computer crime codes, see Paul C. Ray, *Computer Viruses And The Criminal Law: A Diagnosis And A Prescription*, 7 GA. ST. U. L. REV. 455 (1991).

130. Branscomb, *supra* note 129, at 32. *See, e.g.*, MONT. CODE ANN. § 45-6-311 (1993 & Supp. 1994) ("unlawful use of computer" defined as an offense against property, in the section of the code relating to theft); MASS. GEN. LAWS ANN. ch. 266, § 30(2) (West 1990) (larceny statute provides that "[t]he term 'property'. . . shall include . . . electronically processed or stored data, either tangible or intangible, [and] data while in transit"); NEV. REV. STAT. ANN. § 205.4755 (Michie 1992) ("property" includes "information, electronically produced data, program[s], and any other tangible or intangible item of value").

131. Branscomb, *supra* note 129, at 33. *See, e.g.*, IDAHO CODE § 18-2202(2) (1987) (liability attaches to "[a]ny person who knowingly and without authorization alters, damages, or destroys any computer, computer system, or computer network . . . or any computer software, program, documentation, or data contained in such computer, computer system, or computer network."); MD. ANN. CODE art. 27, § 146(c)(2) (1993) (proscribing acts which "[a]lter, damage, or destroy data or a computer program").

132. Branscomb, *supra* note 129, at 34. *See, e.g.*, HAW. REV. STAT. § 708-891(b) (1985 & Supp. 1992) (a person commits computer fraud by "access[ing] or caus[ing] to be accessed any computer, computer system, computer network, or any of its parts with the intent of obtaining money, property or services by means of embezzlement or false or fraudulent representations"); ARIZ. REV. STAT. ANN. § 13-2316 (1989) (computer fraud requires "the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false of fraudulent pretenses"). *Cf.* COLO. REV. STAT. § 18-17-103(5) (1990 & Supp. 1994) (racketeering activity includes committing, attempting to commit, or conspiring to commit offenses involving computer crimes, as defined in § 18-5.5).

133. Branscomb, *supra* note 129, at 34. *See, e.g.*, ALA. CODE § 13A-8-102 (1994) (unauthorized access, modification, destruction, or disclosure of computer programs or data constitutes a crime against intellectual property); MISS. CODE ANN. §§ 97-45-1, 97-45-9 (1994) (intentional and unauthorized "destruction, insertion or modification," "disclosure, use, copying, taking or accessing" of data,

5. *Knowing, unauthorized use.* These statutes prohibit the act of "accessing" or "using" computer systems beyond the consent of the owner.[134]

6. *Unauthorized copying.* This unusual approach appears to be a close cousin of federal criminal copyright infringement. Few states have defined copying programs and data as a distinct state offense.[135]

7. *Prevention of authorized use.* This approach, taken by approximately one-fourth of the states, outlaws any activity which impairs the ability of authorized users to obtain the full utility of their computer systems. Unauthorized execution of programs which slow down the computer's ability to process information falls under such statutes.[136]

8. *Unlawful insertion or contamination.* These statutes criminalize the highly-publicized "viruses," "worms," and "logic bombs" which may be planted on computers or transmitted over telephone lines or on floppy disks. Unlawful insertion provisions do not require actual "access" of a computer by the offender because the offending programs may be communicated indirectly over networks or on floppy disks by offenders who never use the affected computer.[137]

9. *Computer voyeurism.* Computers contain a wide range of confidential personal information. To protect the public's right to privacy in this

---

computer programs or software, and "confidential or proprietary information in any form or medium when such is stored in, produced by or intended for use or storage with or in a computer, a computer system or a computer network" is an offense against intellectual property).

134. Branscomb, *supra* note 129, at 34. *See, e.g.*, OHIO REV. CODE ANN. § 2913.04 (Anderson 1993) ("[n]o person shall knowingly gain access to any computer . . . without the consent of, or beyond the . . . consent of, the owner"); NEB. REV. STAT. § 28-1347 (1989 & Supp. 1994) (unlawful to "knowingly and intentionally exceed the limits of . . . authorization"); ME. REV. STAT. ANN. tit. 17-A, § 432 (West Supp. 1994) (a person who "intentionally accesses any computer resource knowing that the person is not authorized to do so" is guilty of criminal invasion of computer privacy); IOWA CODE § 716A.2 (1993) (proscribing unauthorized access).

135. Branscomb, *supra* note 129, at 35. *Compare* N.Y. PENAL LAW § 156.30 (McKinney 1988 & Supp. 1995) (the copied material need not be copyrightable; the offender must "deprive[] or appropriat[e] from an owner . . . an economic value or benefit in excess of [$2500]") *with* N.J. REV. STAT. § 2C:20-33 (Supp. 1994) (copying or altering a computer program or computer software is not theft if it is of a retail value of $1000 or less and is not copied for resale) *and* federal criminal copyright enforcement, discussed *supra* note 80 and accompanying text.

136. Branscomb, *supra* note 129, at 35. *See* WYO. STAT. § 6-3-504 (1988) ("crime against computer users" occurs if offender "[d]enies computer system services to an authorized user"); LA. REV. STAT. ANN. § 14:73.4 (West 1986 & Supp. 1994) (an offense against computer users takes place when an authorized user is intentionally denied "the full and effective use of or access to a computer, a computer system, a computer network, or computer services").

137. Branscomb, *supra* note 129, at 35. *See, e.g.*, CAL. PENAL CODE § 502 (Deering 1983 & Supp. 1995) ("computer contaminant" defined to include viruses and worms and other sets of instructions designed to "usurp the normal operation of the computer"); CONN. GEN. STAT. § 53a-251(e) (1993) (unlawful to make or cause to be made an unauthorized display, use, disclosure or copy of data, or add data to data residing within a computer system); DEL. CODE ANN. tit. 11, § 935 (1987 & Supp. 1994) (proscribing "interrupt[ion] or add[ition of] data to data residing within a computer system"); MINN. STAT. § 609.87 (1992 & Supp. 1993) (criminalizing any "[d]estructive computer program" that "degrades performance," "disables," or "destroys or alters" data); W. VA. CODE § 61-3C-8 (Michie 1992) (prohibiting "disruption or degradation of computer services").

information, several states have enacted laws criminalizing unauthorized access to a computer system even if only to examine its contents and not make any changes or extract any data.[138]

10. *"Taking possession."* These provisions prohibit the act of assuming control over a computer system and its contents without authorization.[139]

B. Conflict Between State and Federal Laws

The growth of state computer crime legislation has created conflicts between federal and state authorities in prosecuting computer criminals. State computer crime laws have criminalized broad ranges of conduct including unauthorized access, computer fraud, and theft or misuse of computer programs and user time on shared networks.[140] Those state statutes dealing with theft or misuse of copyrightable material, such as computer programs, raise an immediate federalism issue, as copyright law remains the exclusive domain of the federal government.[141]

In 1993, the Fourth Circuit ruled that the section of Virginia's Computer Crimes Act[142] covering reproduction of a copyrighted computer program was pre-empted by the Federal Copyright Act;[143] thus, only the federal government could prosecute illegal copying of computer software. In ruling for federal pre-emption of the Virginia Act, the court held that the state law's mens rea requirement "does not add an element qualitatively changing the state claim from one of unauthorized copying."[144]

Although few reported cases have considered the conflict between federal copyright law and state computer crime statutes,[145] the reasoning in *Rosciszewski* would probably invalidate several other state laws implicating federal

---

138. Branscomb, *supra* note 129, at 36. *See, e.g.*, MO. REV. STAT. ANN. § 569.095(5) (1986 & Supp. 1993) (computer tampering occurs when a person "[a]ccesses a computer, computer system, or a computer network, and intentionally examines information about another person"); W. VA. CODE § 61-3C-12 (Michie 1992) ("computer invasion of privacy" to "knowingly, willfully, and without authorization access[] a computer or computer network and examine[] any employment, salary, credit or any other financial or personal information relating to any other person"). *But see* KY. REV. STAT. ANN. § 434.845(2) (Michie/Bobbs-Merrill 1985) (unauthorized access, even if obtained fraudulently, "shall not constitute a violation . . . if the sole purpose of the access was to obtain information").

139. Branscomb, *supra* note 129, at 37. *See, e.g.*, WIS. STAT. § 943.70(2)(4) (Supp. 1994).

140. *See supra* part III.A. of this article (overview of state criminal codes).

141. Section 301(a) of the Copyright Act explicitly prohibits states from enacting copyright legislation. 17 U.S.C. § 301(a) (1988). This exercise of legislative power by Congress rests on the Article I, Sec. 8 grant of exclusive authority to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art I, § 8.

142. VA. CODE § 18.2-152.3 (Michie 1988 & Supp. 1994) (criminalizing the conduct of one who uses a computer or computer network, without authority and with the intent to obtain property or services by false pretense or to covert the property of another).

143. Rosciszewski v. Arete Assoc., Inc., 1 F.3d 225, 230 (4th Cir. 1993).

144. *Id.* at 230.

145. Wisconsin v. Corcoran, 522 N.W.2d 226 (Wis. Ct. App. 1994).

intellectual property laws.[146] As one commentator observed, the *Rosciszewski* decision may seriously hamper efforts to prosecute computer criminals.[147] As the volume and economic harm caused by computer crimes grows, state and federal law enforcement resources will be increasingly taxed. *Rosciszewski*, by foreclosing any state prosecution of conduct involving computer software, would put the burden increasingly on a federal legal system which has not actively prosecuted in this area.[148]

C. Prosecution of Computer-Related Crimes

Venue provisions are included in some states' laws regarding computer-related crimes.[149] Some states deem a violation to occur where any act performed in furtherance of the offense occurs, where the victim's residence or principle place of business is located, or where an unlawfully accessed computer system is located. Since modems allow a person who commits a computer crime to access a computer miles away, an offender could conceivably face prosecution in more than one jurisdiction.[150]

However, the highly technical nature of computer crimes and the evidentiary difficulties of proving unauthorized access to or modification of a computer system have led to the result that only a handful of cases involving

---

146. *See* Kenneth E. North, *Copyright Act Snarls Computer Crime Laws*, *The National Law Journal*, Nov. 1, 1993, at S36. For example, Illinois' Computer Crime Prevention Law includes copyrighted information in its definition of property; thus, any criminal conduct involving copyrighted "property" could not be prosecuted under state criminal law. 720 ILCS 5/16D-2(d)(3) (1993).

147. North, *supra* note 146, at S36.

148. *Id.* The virtual absence of reported decisions involving federal prosecutions for criminal software infringement indicates a lack of enforcement in this area. If this is true, then *Rosciszewski* may overburden the federal system. *Id.*

149. ARK. CODE ANN. § 5-41-105 (Michie 1993); DEL. CODE ANN. tit. 11, § 938 (1987); GA. CODE ANN. § 16-9-94 (1992); KY. REV. STAT. ANN. § 434.860 (Michie/Bobbs-Merrill 1985); MISS. CODE ANN. § 97-45-11 (1994); N.H. REV. STAT. ANN. § 638:19 (1986); S.C. CODE ANN. § 16-16-30 (Law. Co-op. 1985); S.D. CODIFIED LAWS ANN. § 43-43B-8 (Supp. 1994); TENN. CODE ANN. § 39-14-603 (1991); VA. CODE ANN. § 18.2-152.10 (Michie 1988); W. VA. CODE § 61-3C-18 (1992).

150. Several venue provisions are particularly broad. *See, e.g.*, GA. CODE ANN. § 16-9-94(4) (1992) (venue exists for violations committed "[i]n any county from which, to which, or through which any use of a computer or computer network was made, whether by wires, electromagnetic waves, microwaves, or any other means of communication").

A person may also face federal prosecution, depending on whether he or she lives in the same state as the computer to which unauthorized access is gained. For example, assume that hacker A lives in state X and hacker B lives in state Y. If both hackers gain unauthorized access to a private, non-financial computer system in state X and both subsequently cause identical damage, A is subject to the laws of state X while B is subject to federal law. They may be subject to very different penalties for identical acts. *See* Michael P. Dierks, *Electric Communications and Legal Change: Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 331-32 (1993) (arguing that although jurisdictional boundaries always create arbitrary legal lines, these lines are particularly arbitrary in the world of cyberspace because the sites of the act and actor may not be the same).

computer-related crime have been prosecuted in state courts,[151] and most have dealt with defining the meaning of the terms used in the statutes.[152] The effect has been that state judges lack precedent in making their decisions.

Despite the extremely limited body of precedent, several state supreme and appellate courts have recently handed down decisions fleshing out the respective computer crime statutes of their states.[153] These decisions reflect

---

151. Between 1978 and 1986, there were fewer than 200 prosecutions. Dierks, *supra* note 150, at 329; *see also* Richard Raysman and Peter Brown, *Computer Law: Interpretation of New York's Tampering Statute*, N.Y.L.J., Apr. 12, 1994, at 3. *See generally* People v. Johnson, 560 N.Y.S.2d 238, 241 (N.Y. Crim. Ct. 1990) (information charging defendant for the unauthorized use of a telephone credit card number is facially sufficient since credit card numbers are central to a sophisticated computerized communication system); State v. Moran, 784 P.2d 730, 734 (Ariz. Ct. App. 1989) (defendant did not criminally damage his employer's program by encoding it because he did so with his employer's permission; his refusal to decode was an omission, not an act, and criminal damage is defined in Arizona as a crime of commission, not omission); People v. Weg, 450 N.Y.S.2d 957, 961-62 (N.Y. Crim. Ct. 1982) (allegations that a computer programmer employed by a public agency used his employer's computer for his own commercial benefit with the knowledge that he was not entitled to do so, fail to make out the crime of theft of services, since the computer was not used for profit in trade or commerce, but as an administrative tool).

For other explanations for the lack of diligence in prosecuting computer crimes, see Comment, *The Misuse of Electronically Transferred Confidential Information in Interstate Commerce: How Well Do Our Present Laws Address the Issue?*, 4 SOFTWARE L.J. 529, 552-53 (1991) (the laws may have gaping holes which make enforcement problematic); Hollinger & Lanza-Kaduce, *supra* note 5, at 117 (the laws may be more symbolic than functional); Note, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER L.J. 299, 320-21 (1991) (present laws may be incorrectly conceived). For an interesting discussion of the problems with ex post measures to prevent abuse, see Dierks, *supra* note 142, at 330-36.

152. *See, e.g.*, People v. Versaggi 629 N.E.2d 1034, 1039 (N.Y 1994) (*see infra* note 153 for discussion of case); Gallagher v. State, 618 So. 2d 757, 758 (Fla. Dist. Ct. App. 1993) ("exceeding one's authorized use" is not proscribed as "unauthorized access" under FLA. STAT. § 815.06(1) (1993 & Supp. 1994)); People v. Jemison, 466 N.W.2d 378 (Mich. Ct. App. 1991) (to "cause access to be made" to a computer within the meaning of MICH. COMP. LAWS ANN. § 752.794 (West 1991) requires more than merely supplying information which ultimately finds its way into a computer system in the normal course of business); State v. Lindsly, 808 P.2d 727, 729 (Or. Ct. App. 1991) (investigatory expenses qualify as pecuniary damages under OR. REV. STAT. § 137.103(2) (1990 & Supp. 1994)); Schalk v. State, 767 S.W.2d 441, 448 (Tex. Ct. App. 1988) (defining computer programs as a trade secret).

153. *See* People v. Versaggi, 629 N.E.2d 1034, 1038-39 (N.Y. 1994) (interpreting N.Y. PENAL LAW § 156.20 (McKinney 1988 & Supp. 1995) to uphold the conviction of a former Eastman Kodak computer technician who secretly activated built-in computer commands to shut down the company's telephone system, holding that the legislature also meant to criminalize changes or modifications of the program's intended purpose); Newberger v. Florida, 641 So.2d 419, 421 (Fla. Dist. Ct. App. 1994) (applying *Versaggi*'s interpretation of "alter" in rejecting the defendant's challenge on vagueness grounds of FLA. STAT. § 815.04 (1993 & Supp. 1994), but concluding that defendant, unlike Versaggi, had not used the computer program to do something which changed what the system was designed to do); Washington v. Riley, 846 P.2d 1365, 1373 (Wash. 1993) (finding a telephone company's long-distance switch was a "computer" in upholding the conviction for computer trespass of a hacker who attempted to illegally steal individual long-distance access codes); Pennsylvania v. Gerulis, 616 A.2d 686, 693 (Pa. Super. Ct. 1992), (interpreting the definition of "computer" under 18 PA. CONS. STAT. ANN. § 3933 to encompass voice mailbox systems in upholding the conviction of defendant for secretly using the voice mailbox system of a major hospital to store stolen telephone credit card numbers, because a voice mailbox meets the statutory test that computers are "electronic or high speed data processing device[s] which perform memory functions").

the mix of political and policy concerns state judges face in tackling the unique technical, definitional, and evidentiary problems posed by computer crimes, and may lead courts to place greater emphasis on the net results of a defendant's actions when determining the scope of impermissible access to computer programs and data under computer crime statutes.[154]

IV. INTERNATIONAL APPROACHES

There is general agreement among national governments and multilateral organizations that a coordinated international effort to fight computer crimes is necessary.[155] Many computer systems can be easily and surreptitiously accessed through the global telecommunications network from anywhere in the world.[156] International financial institutions are common targets for computer fraud and embezzlement schemes.[157] The specter of computer terrorism calls for an international strategy to preserve global security.[158]

While "computer crime" remains loosely defined, most industrialized countries have amended their legislation to address four needs created by computer crimes: (1) protection of privacy; (2) prosecution of economic crimes; (3) protection of intellectual property; (4) and procedural provisions to aid in the prosecution of computer crimes.[159] Worldwide, national governments are adopting computer-specific criminal codes that address unauthorized access and manipulation of data, similar to the Computer Fraud and Abuse Act of 1986 in the United States.[160] In general, they have taken three

---

154. *See* Richard Raysman and Peter Brown, *Interpretation of New York's Tampering Statute*, N.Y.L.J., Apr. 12, 1994, at 6.

155. *See generally* Ulrich Sieber, *Computer Crimes and Other Crimes Against Information Technology: Commentary and Preparatory Questions for the Colloquium of the Association Internationale de Droit Pénal in Würzburg* 64 REV. INT'L. DE DROIT. PENAL 67 (1993) (describing international efforts to harmonize computer crime laws).

156. Note, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 TEXAS INT'L L. J. 479, 494 (1992) [hereinafter *Computer-Related Crime*].

157. *See generally* the *Financial Institutions Fraud* and *Securities Fraud* articles in this issue.

158. Thus far, unlawful computer system intrusions have fallen short of disastrous terrorist attacks. However, the potential danger is evident. In one example, a Lithuanian nuclear power plant operator unsuccessfully introduced a virus into the plant's computers, intending to disrupt the nuclear reactor. Nikolai Lashkevich, *Malefactor at Ignalina Nuclear Plant,* SOVIET PRESS DIGEST (Izvestiia), Feb. 3, 1992, at 8.

Computer infiltration may already be an effective weapon of war. United States intelligence agents reportedly planted a computer virus in Iraqi military computers to disable the Iraqi air defense network during the 1991 Persian Gulf War. *Special Report; The Gulf War Flu,* U.S. NEWS & WORLD REP., Jan. 20, 1992, at 50. *Contra Report of Sabotage to Iraq Computer May Be Hoax,* CHI. TRIB., Jan. 14, 1992, at 6.

159. Sieber, *supra* note 155, at 69-70.

160. For reports on computer-crime legislation and prosecution in a number of countries, see Colloquium, *Computer Crime and Other Crimes Against Information Technology*, 64 REV. INT'L DE DROIT PENAL 1 (1993) (reporting on Austria, Belgium, Brazil, Canada, Chile, China, Czechoslovakia, Egypt, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, Luxembourg, the Nether-

approaches in criminalizing computer offenses. First, the "evolutionary" approach simply incorporates computer offenses into existing statutes. Second, "computer-specific offenses" may be defined in terms of existing crimes. Third, "computer-specific statutes" define entirely new crimes.[161]

While a number of differences remain,[162] there are significant areas of convergence in national legislation.[163] By defining specific new offenses and penalties, these codes avoid analytical difficulties that arise when general criminal laws are applied to computer crimes. But even when computer-specific criminal statutes are in place, one commentator suggests that prosecution in a number of industrialized countries will continue to be hindered until the rules of evidence are adapted to computer crimes.[164] When evaluating American computer crime proposals, it is instructive to consider the experiences of other nations.

The Netherlands, for example, passed a strict anti-hacker code in 1992.[165] Dutch computer crime police reported that the number of cases they had to handle doubled from 1991 to 1992.[166] The Dutch law's approach focuses on unauthorized access to secured computer systems. By excluding unsecured systems, the law provides incentives to improve computer security. The penalties provided by the Dutch code vary, depending upon the severity of the intrusion.[167]

---

lands, Poland, Portugal, Romania, South Africa, Spain, Sweden, Switzerland, Tunisia, Turkey, the United Kingdom, and the United States).

161. *Computer-Related Crime*, *supra* note 156, at 494.

162. For example, some European laws focus more on data protection for privacy reasons than do laws in the United States. *See* Comment, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1169-72, 1215-19 (1992)(comparing creation and purpose of U.S. Treasury Department's Financial Crimes Enforcement Network with independent privacy protection agencies in Sweden, Germany and France).

In addition, approaches to prosecuting computer hackers still differ. *See generally* Comment, *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199 (1991)(comparing legislation governing hackers and prosecutions thereunder in Canada, the United States, and the United Kingdom).

163. *See* Cole Durham, *The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm: General Report for the Association Internationale de Droit Pénal Colloquium* 64 REV. INT'L DE DROIT PENAL 79, 97-109 (1993) (discussing patterns of convergence with regard to unauthorized access, unauthorized interception, unauthorized use of a computer, alteration of data or programs, computer sabotage, computer espionage, unauthorized use or reproduction of a computer program, unauthorized reproduction of a topography, computer forgery, and computer fraud).

164. *See generally* Clifford Miller, *Electronic Evidence—Can You Prove the Transaction Took Place?* 9 No. 5 COMPUTER LAW 21 (1992) (analyzing problems of getting evidence of computer crimes admitted under the rules in the United Kingdom as representative of the challenge to prosecutors in the United States, Belgium, Germany and France).

165. *The Netherlands Passes Anti-hacking Law*, COMPUTER FRAUD AND SECURITY BULL., Sept. 1992.

166. *Dutch Police See Hacking Surge*, COMPUTER FRAUD AND SECURITY BULL., Jan. 1993.

167. The Dutch law provides for six months' imprisonment for unauthorized access, up to four years for unauthorized modification, and up to six years for breaking into systems that serve socially

Ultimately, the global interconnection of vulnerable computer systems may require a uniform legal framework for dealing with multi-national computer-related crimes. One possible solution, according to a commentator, is to adopt an international convention standardizing domestic statutes and facilitating cooperative enforcement efforts.[168]

International organizations and private corporations are each working to combat computer crimes. International organizations have worked to harmonize national legislation.[169] Software producers and other providers and users of computer technology are not waiting for international action on computer security. Where nations do not agree to jointly pursue computer criminals, non-governmental organizations are already beginning to fill the void, particularly in the area of computer software piracy.[170] The Business Software Alliance,[171] a software industry trade group, has launched an international copyright enforcement program involving national software trade associations and law enforcement agencies.[172] According to that group, international software piracy costs United States software makers $12 billion dollars annually.[173]

Enforcement programs like these have focused on international distribution of counterfeit software. But as computer criminals become more common, invasions of international computer networks may also prompt greater private-sector initiatives and cooperative efforts between governments.

---

important purposes, such as those of hospitals. James Daly, *Netherlands, Mexico Chase After Hackers*, COMPUTERWORLD, July 13, 1992, at 14.

168. *Computer-Related Crime*, *supra* note 156, at 503-04 (cooperative international solutions could begin on a regional level, such as within the European Community). While the EC's 1991 Software Directive is aimed at harmonizing European copyright laws rather than computer security per se, it does mandate that Member States adopt prescribed penalties for software piracy and procedures for seizing illegally-copied software, a first step towards addressing broader issues raised by computer crimes. Council Directive 91/250/EEC, 1991 O.J. (L122) 42, 42-46.

169. Durham, *supra* note 163, at 97 n.51 (citing efforts by the United Nations, the Council of Europe(301) and the OECD).

170. Criminalization of copyright infringement is gaining momentum around the world. Taiwan and South Korea have indicted companies for illegally copying software for internal use. BUSINESS SOFTWARE ALLIANCE, BSA WORLD-WIDE REPORT 1990-91, Sept. 1991. In Great Britain, software piracy carries prison terms up to two years. BUSINESS SOFTWARE ALLIANCE, UNITED KINGDOM: SOFTWARE PIRACY AND THE LAW. Similar French laws also provide for restitution, doubled penalties for repeat offenders, and court-ordered business closings. BUSINESS SOFTWARE ALLIANCE, FRANCE: SOFTWARE PIRACY AND THE LAW. Singapore provides for up to five years imprisonment for illegally copying software. BUSINESS SOFTWARE ALLIANCE, SINGAPORE: SOFTWARE PIRACY AND THE LAW. *See supra* notes 51-53 and accompanying text (discussing federal criminal copyright infringement). *See generally* the *Intellectual Property* article in this issue.

171. The Business Software Alliance is a Washington, D.C. based organization funded by major software publishers.

172. The Business Software Alliance together with the Mexican federal attorney's office, initiated a 1992 software piracy investigation which led to seizure of illegally reproduced software programs. James Daly, *Netherlands, Mexico Chase After Hackers*, COMPUTERWORLD, July 13, 1992, at 14.

173. *This Lobby Speaks Software and Carries a Big Stick*, BUSINESS WEEK, March 22, 1993, at 88.

V. ANCILLARY ISSUES

In *United States v. Sawyer*,[174] a search warrant listing general categories of business records, including "computer records and printouts relating to customer accounts, which are evidence and fruits of, and the means of commission of violations of [certain U.S. statutes]," withstood Fourth Amendment[175] scrutiny.[176] The court stated that the particularity requirement of the Fourth Amendment must be applied flexibly, and in cases involving a "pervasive scheme to defraud, all the business records of the enterprise may properly be seized."[177] The seizure of computer disks is allowed even when the warrant refers only to records and documents.[178] Police with a warrant to seize records may search computer hardware and software as long as they have reason to believe that the items contain records whose seizure is covered by the warrant.[179] When police conduct such a search, they may seize and examine a disk, even if its label indicates that it does not contain information within the scope of the warrant.[180] The police may take the hardware and software off the premises to conduct their examination.[181] They may not, however, seize peripherals such as printers to assist them in

---

174. 799 F.2d 1494 (11th Cir.), *cert. denied*, 479 U.S. 1069 (1986).

175. The Fourth Amendment states that " . . . no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

176. *Sawyer*, 799 F.2d at 1509. *Cf.* Washington v. Riley, 846 P.2d 1365, 1369 (Wash. 1993) (invalidating as overbroad a search warrant permitting the seizure of broad categories of computer records without specifying the crimes being investigated).

177. *Sawyer*, 799 F.2d at 1508.

178. United States v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986).

179. *See* United States v. Sissler, No. 1:90-CR-12, 1991 U.S. Dist. LEXIS 16465, at *11 (W.D. Mich. Aug. 30, 1991) (because police "are permitted to search any container found within the premises if there is reason to believe that the evidence sought pursuant to a warrant is in it . . . police [are] permitted to examine the computer's internal memory and the disks since there was every reason to believe that they contained records whose seizure was authorized by the warrant") (citing United States v. Ross, 456 U.S. 798, 820-21 (1982)). *Cf.* United States v. Ponce, No. 91-50256, 1993 U.S. App. LEXIS 7462, at *10-11 (9th Cir. Apr. 1, 1993) (affirming admission of printout made from computer disk seized in a search on the grounds that the disk, from which the printout was made, contained a drug ledger and was found at the defendant's home).

180. *Sissler*, 1991 U.S. Dist. LEXIS 16465, at *11-12 ("the police were not obligated to give deference to the descriptive labels placed on the discs . . . . Otherwise, records of illicit activity could be shielded from seizure by simply placing an innocuous label on the computer disk containing them.").

181. *Id.* at *12.

> [The] police also were not obligated to inspect the computer and disks at the . . . residence because passwords and other security devices are often used to protect the information stored in them. Obviously, the police were permitted to remove them . . . so that a computer expert could attempt to 'crack' these security measures, a process that takes some time and effort.

Id.

their review of the seized items.[182] Finally, assistance of advisers to identify computer-related items encompassed by a search warrant is permissible.[183]

An interesting overlap exists between Fourth Amendment and First Amendment[184] issues. The question for debate is whether electronic data constitutes speech, and whether a computer which disseminates this data to the public can be considered a "newspaper" which enjoys the freedoms protected by the First Amendment and the Privacy Protection Act of 1980.[185]

MICHAEL W. CARROLL
ROBERT SCHRADER

182. *Id.* at *12 n.7.

183. State v. Wade, 544 So. 2d 1028, 1030 (Fla. Dist. Ct. App. 1989) (permitting use of competitor's employees to identify items).

184. The First Amendment states, in part, that "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . " U.S. CONST. amend. I.

185. 42 U.S.C. §§ 2000aa to 2000aa-12 (1988). The Privacy Protection Act explicitly includes "mechanically, magnetically or electronically recorded cards, tapes, or discs" in its definition of "documentary materials." *Id.* § 2000aa-7(a) (1988). This issue was considered in Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994). The court ruled that the Secret Service was in violation of the Act when it seized computer media, including floppy and hard disks, because these materials were possessed in anticipation of communicating the materials to the public. *Id.* at 440-41.